ANONOS

Schrems II – Data Embassy for Cloud

On 16 July 2020, the highest court in the EU, the Court of Justice of the European Union (CJEU), issued a final, unappealable ruling known as “Schrems II” which invalidated the EU-US Privacy Shield for international data transfers.

Previously, some companies engaged in “regulatory arbitrage” by choosing not to comply with privacy laws and baking the cost of non-compliance into their cost of doing business. Of great significance under Schrems II is that the CJEU ruled that unlawful international data transfer processing must be *stopped*, rather than fined. This makes a “regulatory arbitrage” approach impossible – lack of access to data halts business operations, and cannot be merely calculated into the cost of doing business.

Since the Schrems II decision, it has become increasingly clear that the location of servers supporting US-based cloud providers is immaterial under Schrems II. This is because the operations of these firms fall under the jurisdiction of US laws (e.g. the Foreign Intelligence Surveillance Act or "FISA” and the Cloud Act of 2018) which enable federal law enforcement officials to compel US-based technology companies to provide requested data stored on servers regardless of where the servers are located. This means it does not matter whether they are located in the US or on foreign soil. Examples of such clarifications include:

- Recommendation by the French Data Protection Authority, the CNIL, that French Health Data Hub information should not be hosted by cloud companies under US jurisdiction;
- Review of the UK Government Digital Service (GDS) Cloud First policy due to the Schrems II invalidation of the EU-US Privacy Shield arrangement and reliance on US-based providers.
- Guidance by a German Data Protection Regulator that EU entities cannot lawfully transfer data to cloud or other technology providers not organized under the laws of the EU, European Economic Area or an equivalent protection country, making providers from the US, UK, India and other countries unlawful.
- Clarification by the European Data Protection Board (EDPB) that the term “transfer” for purposes of Schrems II includes “providing access to data from a third country, for instance for administration purpose [or] for storage or maintenance purposes.”

However, the CJEU also ruled in Schrems II that contract-based Standard Contractual Causes (SCCs) and internal Binding Corporate Resolutions (BCRs) may continue to be used to support lawful international data transfers (including the use of US-based cloud providers) if adequate “supplementary measures” are in place to ensure protection consistent with EU data protection laws.

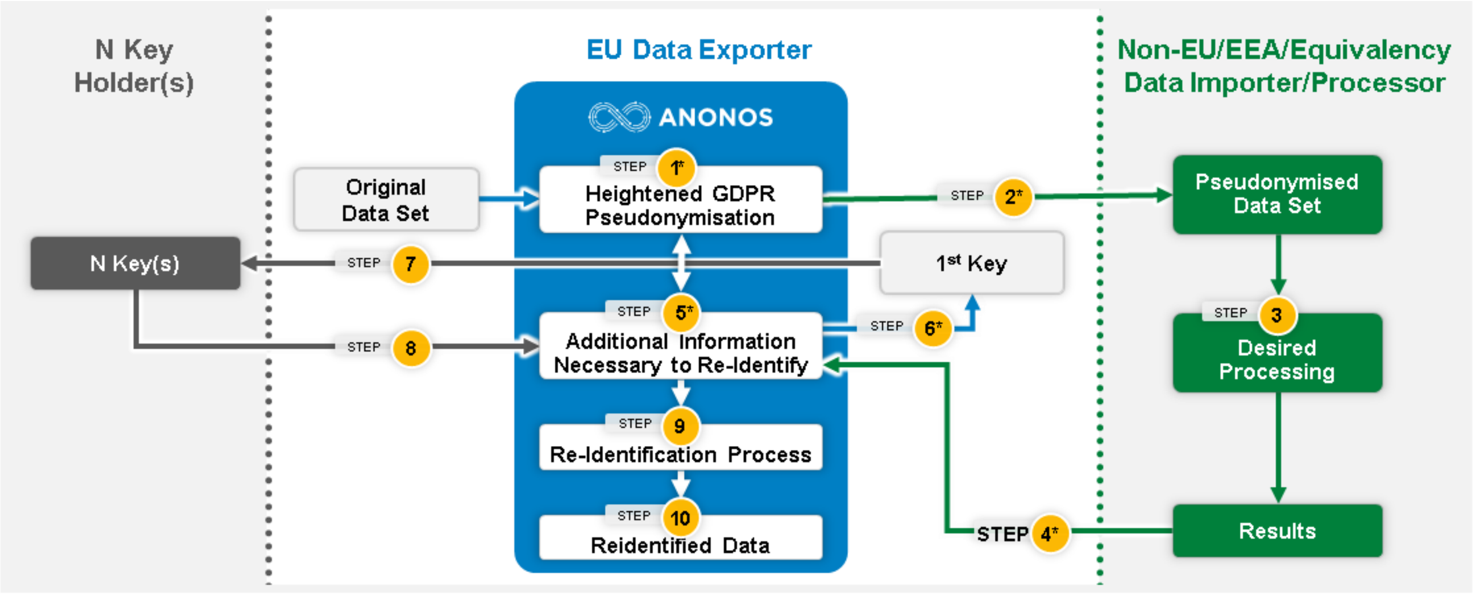
To comply with Schrems II SCC/BCR requirements, Anonos software enforces Data Embassy principles (DataEmbassy.com) that embody EU data protection rules to create privacy-secured versions of data called Variant Twins. These Variant Twins leverage GDPR-heightened requirements for Pseudonymisation, alongside Anonos patented proprietary techniques. Variant Twins prevent re-identification of individuals by national authorities without access to additional information that is held by the EU exporter. If a US-based cloud provider or other data importer processing Variant Twin data is subpoenaed, the importer would not be in a position to help US law enforcement or the Department of Justice to re-identify the data. Rather, they would have to go to the EU exporter for the “additional information” required for re-identification. Under EU and national laws, these exporters have an affirmative obligation to prioritize compliance with EU data protection regulations and resist foreign production requests. A graphical depiction of enforcing Data Embassy principles using Anonos Variant Twins is below.

Anonos enables organizations to leverage investments in cloud transformation journeys involving US-owned or operated cloud-based IaaS and SaaS capabilities (e.g. AWS, Azure, GCP, IBM and Oracle) in compliance with new requirements under Schrems II by ensuring the fundamental rights of data subjects.

For more information, visit SchremsII.com/learn

Contact us at DataLiquidity@anonos.com for information on how Anonos Data Liquidity enables you to continue lawful international data transfers and processing, using cloud, SaaS and outsourcing arrangements.

Anonos Variant Twin Enforcement of Data Embassy Principles To Comply with Schrems II by Ensuring Fundamental Rights


N Key Holder(s)
EU Data Exporter
Non-EU/EEA/Equivalency Data Importer/Processor
ANONOS
Original Data Set
STEP 1* Heightened GDPR Pseudonymisation
STEP 2*
Pseudonymised Data Set
N Key(s)
STEP 7
1st Key
STEP 5* Additional Information Necessary to Re-Identify
STEP 6*
STEP 3 Desired Processing
STEP 8
STEP 9 Re-Identification Process
STEP 10 Reidentified Data
STEP 4*
Results

* May be performed by an EU/EEA/Equivalency service provider on behalf of the EU Data Exporter

1 The EU Data Exporter creates a Pseudonymised Data Set using patented Anonos Dynamic De-Identification (DDID) capabilities.[1]

2 The Pseudonymised Data Set is provided to a third party (e.g., non-EU, EEA or Equivalency Country cloud, SaaS or outsourcing provider) for processing.

3 The desired processing of the Pseudonymised Data Set is performed.

4 The results of the processing are returned to the EU Data Exporter.

5 The EU Data Exporter retains possession of the “additional information” necessary to relink GDPR-compliant Pseudonymised data back to the source identifying data used to create the Pseudonymised data.

6 The “1st Key” required to access this “additional information” resides with the EU Data Exporter. Without access to this 1st Key, the “additional information” is not accessible by anyone and the GDPR-compliant Pseudonymised data is not capable of being re-identified. The “1st Key” is created, updated and maintained using Anonos Dynamic De-Identification (DDID) capabilities.

7 OPTIONAL: access to the “additional information” requires use of one or more additional “N-Keys” held by other parties.

8 The EU Data Exporter (i) either holds the only 1st Key by themselves or (ii) must combine their key with one or more additional “N Keys” required to access and use the “additional information.” The “N Keys” are created, updated and maintained using Anonos Dynamic De-Identification (DDID) capabilities.[2]

9 The “additional information” is used to reverse the Pseudonymisation process.

10 The reidentified data is available for authorized processing.

[1] Anonos Dynamic De-Identification (DDID) capabilities are protected by an international patent portfolio including Patents: CA 2,975,441 (2020); EU 3,063,691 (2020); US 10,572,684 (2020); CA 2,929,269 (2019); US 10,043,035 (2018); US 9,619,669 (2017); US 9,361,481 (2016); US 9,129,133 (2015); US 9,087,216 (2015); and US 9,087,215 (2015). Note that in certain implementations, Steps 1, 2, 4, 5 and/or 6 could be performed by an EU/EEA/Equivalency service provider on behalf of the EU Data Exporter.

[2] In certain implementations, a non-EU, EEA or Equivalency Country cloud, SaaS or outsourcing service provider might be authorized to serve as one (of several) N Key holders so long as sufficient guarantees of non-surveillance remain in effect. Upon failure of such guarantees, another party authorized as an N Key holder (e.g., another party within the EU Data Exporter, an EU/EEA/Equivalency service provider, a trusted third party, a court of competent jurisdiction, etc.) would provide their N Key to enable access to and use of “additional information.”

Contact us at DataLiquidity@anonos.com for information on how Anonos Data Liquidity enables you to continue lawful international data transfers and processing, using cloud, SaaS and outsourcing arrangements.